UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/650,440	08/27/2003	Frederic G. Thiele	END920030068US1	7247

26502 7590 12/10/2010

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2432	

NOTIFICATION DATE	DELIVERY MODE
12/10/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

endiplaw@us.ibm.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte FREDERIC G. THIELE and MICHAEL A. WALTER

Appeal 2009-007294
Application 10/650,440[1]
Technology Center 2400

Before JEAN R. HOMERE, ST. JOHN COURTENAY III,
CAROLYN D. THOMAS, *Administrative Patent Judges.*

HOMERE, *Administrative Patent Judge.*

DECISION ON APPEAL[2]

---

[1] Filed on August 27, 2003. The real party in interest is International Business Machines Corp. (Br. 1; Ans. 2.)

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) (2002) from the Examiner's final rejection of claims 1 through 16 and 21 through 24. (Br. 1.) Claims 17 through 20 have been cancelled. (*Id.*) We have jurisdiction under 35 U.S.C. § 6(b) (2008).

We affirm.

Appellants' Invention

Appellants invented a computer program product and system for detecting unknown computer attacks by automatically determining if a data packet is an exploit candidate (i.e., new computer viruses, worms, exploitation programs, etc.). (Spec. 1, ll. 4-5; *id.* at 4, ll. 12-13; *id.* at 7, l. 29- *id.* at 8, l. 1.)

Illustrative Claim

Independent claim 1 further illustrates the invention as follows:

> 1. A computer program product for automatically determining if a packet is a new, exploit candidate, said program product comprising:
>
> a computer readable medium;
>
> first program instructions to determine if said packet is a known exploit or portion thereof;
>
> second program instructions to determine if said packet is addressed to a broadcast IP address of a network; and
>
> third program instructions to determine if said packet is network administration traffic
>
> fourth program instructions, responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, or network administration traffic to determine that said packet is not a new, exploit candidate; and

fifth program instructions, responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or another type of traffic known to be benign, to determine and report that said packet is a new, exploit candidate; and wherein

said first, second, third, fourth and fifth program instructions are embodied on said medium.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Amit	2002/0116512 A1	Aug. 22, 2002
Hasegawa	2002/0131369 A1	Sep. 19, 2002
Suuronen	2003/0145228 A1	Jul. 31, 2003
Grenot	6,853,619 B1	Feb. 8, 2005 (PCT filed Feb. 9, 2000)

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

Claims 1, 2, 4, 5, 7, 12 through 15, 21, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Suuronen and Amit.[3]

---

[3] In the Final Rejection entered March 5, 2007, the Examiner appears to have rejected dependent claim 7 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Suuronen and Amit. However, we note that dependent claim 6, from which claim 7 depends, stands rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Suuronen, Amit, and Hasegawa. Therefore, we will treat dependent claim 7 as being rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Suuronen, Amit, and Hasegawa. Since Appellants failed to separately argue this on appeal, Appellants have waived any such arguments. *See In re Watts*, 354 F.3d 1362, 1367 (Fed. Cir. 2004).

Claims 3, 8 through 11, and 24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Suuronen, Amit, and Grenot.

Claims 6, 16, and 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Suuronen, Amit, and Hasegawa.

Appellants' Contentions

Appellants contend that Suuronen discloses a virus scanning engine that works in conjunction with a bypass/screening system that screens each data packets to determine if it contains a virus. Upon determining that a data packet does not contain a virus, Suuronen's disclosed system allows the data packet to bypass the virus scanning engine. (Br. 6.) Therefore, Appellants argue that Suuronen fails to disclose the claimed second, third, fourth, and fifth program instructions. (*Id.*) Appellants also allege that Suuronen discloses utilizing virus detection criteria specified by a virus detection database in order to determine which packets should pass through or bypass a virus scanning engine. (Br. 7.) In particular, Appellants contend that Suuronen's virus scanning engine does not identify new, exploit candidates that do not exist in the virus detection database. (*Id.*) Appellants also argue that Amit's disclosure fails to identify any new, exploit candidates. (*Id.* at 7-8.) Further, Appellants contend that there is no reason to combine Suuronen and Amit because each reference addresses a different task and problem, which pertains to a different technology involving a different technician. (*Id.* at 8.)

Examiner's Findings and Conclusions

The Examiner finds that Suuronen discloses a gateway that filters packets between the Internet and a Local Area Network ("LAN"). (Ans. 8.)[4] In particular, the Examiner finds that Suuronen's LAN comprises many users that can receive packets broadcasted from the gateway. (*Id.*) Therefore, the Examiner finds that Suuronen's disclosure teaches determining if a packet is addressed to a broadcast IP address of a network. (*Id.*) Further, the Examiner finds that Suuronen discloses utilizing a packet classification database in order to classify incoming packets as a first and second type. (*Id.*) The Examiner finds that Suuronen's first packet type is known to be virus free and can be readily passed to a destination. (*Id.*) Moreover, the Examiner finds that Suuronen's first packet type contains information for setting up transmission sessions to other ports. (*Id.* at 8-9.) Therefore, the Examiner finds that Suuronen's information pertaining to setting up transmissions to other ports amounts to a network administration function. (*Id.* at 9.)

Additionally, the Examiner finds that Suuronen's disclosure of screening a second packet type against a virus detection database, which is capable of being updated in order to identify new and changing threats (i.e., viruses), teaches identifying viruses contained within the system. (*Id.*) The Examiner also finds that Amit's disclosure of detecting and classifying packets as primary or secondary packets teaches identifying new, exploit candidates. (*Id.* at 9-10.) Finally, the Examiner finds that both Suuronen

[4] All references to the Examiner's Answer are to the Answer filed on December 5, 2007, which replaced the prior Answer filed on November 14, 2007.

and Amit pertain to similar tasks because Suuronen discloses network security through surveillance of packets and Amit discloses surveillance of packets for security reasons. (*Id.* at 10.)

II. ISSUES

Have Appellants shown that the Examiner erred in concluding that the combination of Suuronen and Amit renders independent claim 1 unpatentable? In particular, the issue turns on whether:

(a) the proffered combination teaches "second program instructions to determine if said packet is addressed to a broadcast IP address of a network," as recited in independent claim 1;

(b) the proffered combination teaches "third program instructions to determine if said packet is network administration traffic," as recited in independent claim 1;

(c) the proffered combination teaches "fourth program instructions, responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, or network administration traffic to determine that said packet is not a new, exploit candidate," as recited in independent claim 1;

(d) the proffered combination teaches "fifth program instructions, responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or another type of traffic known to be benign, to determine and report that said packet is a new, exploit candidate," as recited in independent claim 1; and

(e) Suuronen and Amit are analogous art and can be properly used in the proffered combination.

III. FINDINGS OF FACT

The following Findings of Fact ("FF") are shown by a preponderance of the evidence.

Suuronen

1. Suuronen discloses detecting the presence of a computer virus in data transmissions to various networks. (1: ¶ [0002].)

2. Suuronen's figure 1 depicts a virus protection system (10). (2: ¶ [0019].) In particular, Suuronen disclose a firewall (12) that utilizes a packet classification database (16) and corresponding criteria to classify data packets as a first type which does not contain a virus. (*Id.*) Suuronen discloses transmitting data packets of a first type from the firewall (14) to their respective destinations set forth within the network architecture. (*Id.*) Suuronen also discloses that the firewall (14) transmits data packets classified as a second type, which may contain a virus, to a virus scanning engine (22) for further analysis. (*Id.*)

Amit

3. Amit discloses enabling surveillance and monitoring of network communications by analyzing data transmitting through a network. (1: ¶ [0001].)

Grenot

4. Grenot's figure 3 depicts the internal functional organization of a system. (Col. 4, ll. 43-45.) In particular, Grenot's figure 3 depicts

classification of packets (11) and filtering packets based on such classification (45). (*See* figure 3.)

IV. ANALYSIS

Claim 1

Independent claim 1 recites, in relevant parts:

> 1) second program instructions to determine if said packet is addressed to a broadcast IP address of a network; 2) third program instructions to determine if said packet is network administration traffic; 3) fourth program instructions, responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, or network administration traffic to determine that said packet is not a new, exploit candidate; and 4) fifth program instructions, responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or another type of traffic known to be benign, to determine and report that said packet is a new, exploit candidate.

As detailed in the Findings of Fact section above, Suuronen discloses detecting the presence of a computer virus in a data transmission. (FF 1.) In particular, Suuronen discloses a virus protection system that includes a firewall which classifies data packets that do not contain a computer virus as a first type, and transmits such packets to a destination within a network. (FF 2.) Suuronen also discloses that the firewall classifies data packets that may contain a virus as a second type, and transmits such packets to a virus scanning engine for further analysis. (*Id.*)

We find that Suuronen's disclosure teaches a virus protection system that determines whether a data packet contains a virus, and classifies the data packet as a first type (i.e., a data packet that does not contain a computer

virus) or a second type (i.e., a data packet that may contain a computer virus). We also find that Suuronen's disclosure teaches transmitting the data packet to either a destination within the network or a virus scanning engine based on the respective classification. In particular, we find that an ordinarily skilled artisan would have appreciated the fact that Suuronen's disclosure of classifying a data packet as a first type or second type amounts to determining if the data packet is a known computer virus. Further, if the data packet is a known computer virus, an ordinarily skilled artisan would have understood that the data packet is not a new computer virus.

Additionally, we note that the fourth and fifth program instructions are claimed in the alternative and, therefore, Suuronen's disclosure only needs to teach or fairly suggest one of the alternatives. Accordingly, we find that Suuronen's disclosure of determining if a data packet is a known computer virus (i.e., not a new computer virus) teaches or fairly suggests "fourth program instructions, responsive to said packet being known exploit or portion thereof, addressed to a broadcast IP address of a network, or network administration traffic to determine that said packet is not a new, exploit candidate," as recited in independent claim 1. Moreover, we find that Suuronen's disclosure of determining that a data packet is not a known computer virus, but instead a potentially new computer virus, teaches or fairly suggests "fifth program instructions, responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or another type of traffic known to be benign, to determine and report that said packet is a new, exploit candidate," as recited in independent claim 1.

We are not persuaded by Appellants' argument that Suuronen's disclosure fails to teach or fairly suggest "second program instructions to determine if said packet is addressed to a broadcast IP address of a network," and "third program instructions to determine if said packet is network administration traffic," as recited in independent claim 1. (Br. 6-7.) We note that Appellants' attempt to distinguish the second and third program instructions over Suuronen based upon the nature of the information contained or stored in the claimed "packet" is unavailing. Appellants cannot rely solely upon the content or type of information stored in the claimed "packet" to patentably distinguish independent claim 1 over the prior art of record. The content or type of such information is non-functional descriptive material, which is not entitled to any patentable weight. *See In re Lowry*, 32 F.3d 1579, 1583 (Fed. Cir. 1994) ("Lowry does not claim merely the information content of a memory…. Nor does he seek to patent the content of information resident in a database."). *See also Ex parte Nehls*, 88 USPQ2d 1883, 1887-90 (BPAI 2008) (precedential); *Ex parte Curry*, 84 USPQ2d 1272, 1274-75 (BPAI 2005) (informative), aff'd, slip op. 06-1003 (Fed. Cir. June 2006) (Rule 36).

Analogous Art

We are not persuaded by Appellants' argument that Suuronen and Amit are non-analogous art and cannot be properly used in the proffered combination. (Br. 8.) "Whether a reference in the prior art is analogous' is a fact question." *In re Clay*, 966 F.2d 656, 658 (Fed. Cir. 1992) (citing *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1568 n.9 (Fed. Cir. 1987)).

> Two criteria have evolved for answering the question: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.

Id. at 658-59 (citing *In re Deminski*, 796 F.2d 436, 442 (Fed. Cir. 1986); *In re Wood*, 599 F.2d 1032, 1036 (CCPA 1979)).

We find that both Suuronen and Amit reasonably pertain to the problem with which Appellants were concerned at the time of the claimed invention. In particular, Appellants sought to detect unknown computer attacks by utilizing a program to filter out data packets that are not new computer viruses. (Spec. 1, ll. 3-4; *id.* at 10, ll. 7-10.) Similarly, Suuronen is concerned with detecting the presence of a computer virus in data transmissions to various networks. (FF 1.) Moreover, Amit pertains to enabling surveillance and monitoring of network communications by analyzing data transmitting through the network. (FF 3.) Thus, we find that an ordinarily skilled artisan would have recognized that both Suuronen and Amit are directed to the problem of detecting attacks on computer systems by monitoring data packets traversing through a network, which is the same problem that Appellants were concerned with at the time of the claimed invention. It follows that Appellants have not shown that the Examiner erred in concluding that the combination of Suuronen and Amit renders independent claim 1 unpatentable.

Claims 2, 6, 14, 16, 22, and 23

Appellants generally allege that the proffered combinations fail to teach the respective limitations recited in dependent claims 2, 6, 14, 16, 22, and 23. (Br. 9, 13-15.) Appellants are reminded that merely reiterating what

a claim recites or making a general allegation of patentability is not a separate patentability argument. *See Ex parte Belinne*, No. 2009-004693, slip op. at 7-8 (BPAI Aug. 10, 2009) (informative); *see also* 37 C.F.R. § 41.37(c)(1)(vii). Therefore, Appellants' arguments are unpersuasive. It follows that Appellants have not shown that the Examiner erred in concluding that the combination of Suuronen and Amit renders dependent claims 2, 14, and 22 unpatentable, and the combination of Suuronen, Amit, and Hasegawa renders dependent claims 6, 16, and 23 unpatentable.

Claims 3 through 5, 7, 8, 10 through 13, and 15

Appellants do not provide separate arguments for patentability with respect to independent claim 13, and dependent claims 3 through 5, 7, 8, 10 through 13, and 15. Therefore, we select independent claim 1 as representative of the cited claims. Consequently, Appellants have not shown error in the Examiner's rejection of independent claim 13, and dependent claims 3 through 5, 7, 8, 10 through 13, and 15, for the reasons set forth in our discussion of independent claim 1. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Claim 9

Appellants contend that Suuronen, Amit, and Grenot fail to teach "determine[ing] if said packet has a protocol listed in a list of protocols assumed to be harmless network broadcast traffic," as recited in dependent claim 9. (Br. 10.) Further, Appellants argue that Grenot fails to teach or suggest a program or algorithm for determining new, exploit candidates. (*Id.*) Appellants also allege that although Grenot discloses identifying various IP addresses associated with a packet, Grenot fails to disclose the claimed program operations, as recited in independent claim 1. (*Id.*) Additionally, Appellants contend that there is no reason to combine

Suuronen, Amit, and Grenot because each reference addresses a different task and problem, which pertains to different technology involving a different technician. (*Id.* at 10-11.) We do not agree.

As set forth above, Suuronen's disclosure teaches a virus protection system that determines whether a data packet contains a virus by classifying the data packet as a first or second type and, subsequently, transmits the data packet accordingly. In particular, we find that an ordinarily skilled artisan would have appreciated that Suuronen's disclosure of classifying a data packet as a first type (i.e., a data packet that does not contain a virus) amounts to determining that the data packet contains a protocol that is assumed to be harmless network broadcast traffic. Thus, we find that Suuronen's disclosure teaches or fairly suggests the disputed limitation.

Analogous Art

As set forth above, we find that the claimed invention detects unknown computer attacks by utilizing a program to filter out data packets that are not new computer viruses. (Spec. 1, ll. 3-4; *id.* at 10, ll. 7-10.) In particular, we find that Appellants' field of endeavor pertains to determining potential computer attacks by filtering data packets. Similarly, Grenot discloses classifying data packets and filtering data packets based on such classification. (FF 4.) Therefore, we find that Grenot is within the same field of endeavor as the claimed invention because they are both concerned with filtering data packets.

Nonetheless, as set forth above, Suuronen's disclosure teaches the disputed limitation. It follows that Appellants have not shown that the Examiner erred in concluding that the combination of Suuronen, Amit, and Grenot renders dependent claim 9 unpatentable.

Claims 21 and 24

Appellants offer the same arguments set forth in response to the obviousness rejection of dependent claim 9, to rebut the obviousness rejection of independent 21. (Br. 13.) We have already addressed these arguments in our discussion of dependent claim 9 and we found them unpersuasive. Consequently, Appellants have not shown that the Examiner erred in concluding that the combination of Suuronen and Amit renders independent claim 21 unpatentable.

Appellants do not provide separate arguments for patentability with respect to dependent claim 24. Therefore, we select independent claim 21 and dependent claim 9 as representative of the cited claim. Consequently, Appellants have not shown error in the Examiner's rejection of dependent claim 24 for the reasons set forth in our discussion of independent claim 21 and dependent claim 9. *See* 37 C.F.R. § 41.37(c)(1)(vii).

V. CONCLUSION OF LAW

Appellants have not shown that the Examiner erred in rejecting claims 1 through 16 and 21 through 24 as being unpatentable under 35 U.S.C. § 103(a).

VI. DECISION

We affirm the Examiner's decision to reject claims 1 through 16 and 21 through 24.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED

Vsh

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760